USE CASE | Energy

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

IDENTITY AND ACCESS MANAGEMENT

Securing Networked Infrastructure for the Energy Sector

The National Cybersecurity Center of Excellence (NCCoE), in collaboration with energy sector stakeholders and cybersecurity vendors, has developed an example identity and access management (IdAM) solution. The solution provides a demonstration of commercially available technologies that support a converged IdAM platform. This platform follows both standards and best practices, and is informed by NERC CIP version 5 rules. If you would like to utilize the design or view a demonstration, please contact us at energy_nccoe@nist.gov.

THE CHALLENGE

As the electric power industry upgrades infrastructure to take advantage of emerging technologies, utilities are also moving towards greater information technology (IT) and operational technology (OT) convergence. This allows technologies, devices, and systems to connect to the grid to improve efficiency, provide access to data normally held in silos, and enhance productivity. One such area that touches a utility's IT and OT departments is identity and access management (IdAM), which manages access to networked resources, including buildings, equipment, technology and industrial control systems.

Many utilities run decentralized IdAM systems managed by separate departments. Employees who manage these systems often lack time and methods to coordinate access to devices and facilities across IT and OT silos. This creates inefficiency and can result in security risks for utilities, according to our electric sector stakeholders. Additionally, a decentralized IdAM platform spread across separate silos in a utility can lead to an increased risk of attack and service disruption, an inability to identify potential sources of a problem or attack, and a lack of overall traceability and accountability regarding who has access to both critical and noncritical assets.

THE SOLUTION

A converged IdAM platform can provide a comprehensive view of all users and their access rights across the enterprise. The NCCoE used commercially available technologies to develop an example converged IdAM solution that utilities can use to increase security and efficiency in managing access to their networked devices and facilities.

The work and development of this example solution is documented in NIST Cybersecurity Practice Guide, Special Publication 1800-2: "Identity and Access Management for Electric Utilities." Utilities can use some or all of the guide to implement a converged IdAM system using NIST and industry standards, including the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards. Commercial, standards-based products, like the ones the NCCoE used, are easily available and interoperable with commonly used infrastructure.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCoE
Visit http://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

THE BENEFITS

The NCCoE's example IdAM solution details products and capabilities that can be adopted on a component-by-component basis, or as a whole, thereby minimizing impact to the enterprise and existing infrastructure. The example solution:

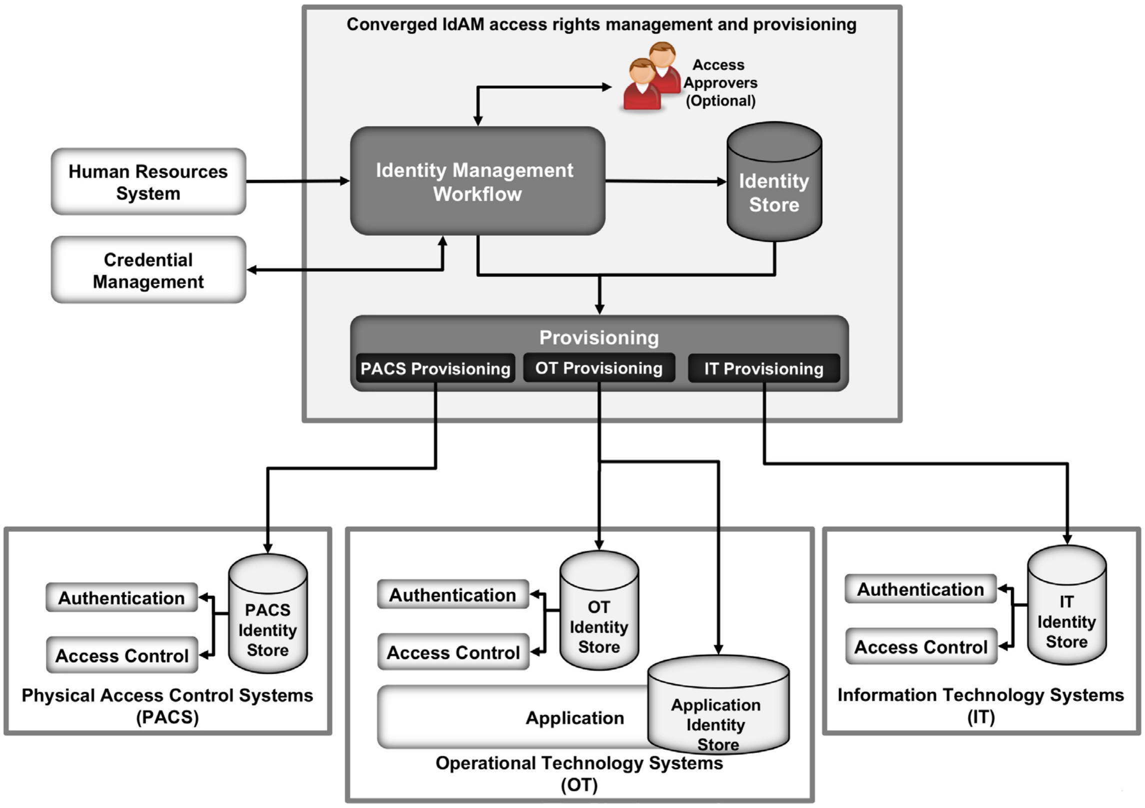
- can reduce the risk of malicious or untrained people gaining unauthorized access to critical infrastructure components and interfering with their operation, thereby lowering overall business risk
- allows rapid provisioning and de-provisioning of access from a converged platform
- simplifies regulatory compliance by automating generation and collection of access information
- improves situational awareness: proper access and authorization can be confirmed via the use of a single, converged solution
- improves security posture by tracking and auditing access requests and other IdAM activity across all networks
- can enhance the productivity of employees, support oversight of resources, and speed delivery of services

IMPLEMENTATION OVERVIEW

Our example solution includes components such as:

- services for authenticating and authorizing users based on identity and role
- services for authenticating and authorizing devices
- an identity and access governance capability that translates human-readable access needs into machine-readable authorizations
- industrial control systems equipment, such as remote terminal units, programmable logic controllers, and relays, along with associated software and communications equipment (e.g., routers and firewalls)
- physical access control devices that use standard communication interfaces
- "bump-in-the-wire" devices for augmenting operational technology with authentication, authorization, access control, encrypted communication and logging capabilities

ARCHITECTURE



DOWNLOAD THE PRACTICE GUIDE

Visit https://nccoe.nist.gov/projects/use_cases/idam to learn more about this project.

HOW TO PARTICIPATE

Share your thoughts on the relevance of this guide, or join our pilot program to launch a similar converged IdAM system in your organization. Contact us at energy_nccoe@nist.gov.

August 2016